	COUNTY OF SAN BERNARDINO POLICY	No. 2-364 Issue No. 1 Effective: May 24, 2006 Page 1 of 2 By: Bea Valdez, Chief of Administrative Services
	PUBLIC HEALTH	Approved: James A. Felten Public Health Director
Subject: SYSTEMS ACCESS CONTROLS		

I. POLICY:

It is the policy of the Department of Public Health (DPH) to protect systems, resources, and data from unauthorized access and to determine the appropriate level of DPH workforce member access by establishing access controls. DPH shall implement a process for authorizing users' access rights that is auditable, traceable and demonstrates effective control over the granting of access privileges.

II. PURPOSE:

This policy establishes guidelines for DPH workforce members for controlling access to automated systems through the issuance of system User-IDs and passwords.

III. DEFINITIONS

A. Access: Access to Information Technology (IT) systems is permitted or denied to individuals based on their job requirements. This access is controlled by the use of a User-ID.

B. Unique User-IDs: Each individual system or application requires a unique User-ID that serves as an identifier to that system so that access rights can be granted appropriately.

C. User Authentication: Associated with the User-ID, each individual system or application will require a password to ensure that only authorized users are granted access.

D. Automatic Logoff: Automatic system logoff will occur after a predetermined period of inactivity.

IV. SCOPE:

A. Managers' Responsibilities:

1. Authorize DPH information access rights for each workforce member.
2. Ensure that workforce members have access to and have read County and DPH security policies and practices.
3. Ensure that access rights to DPH information are adjusted when a workforce member separates from DPH, assumes different responsibilities, or transfers to another department.
4. Ensure that any exceptions to this policy are documented and approved by DPH Administration and IT.

B. Workforce Members' Responsibilities:

1. Read and comply with all County and DPH security policies and practices.
2. Protect the confidentiality of all systems access passwords and User-IDs.
3. Access only the information needed to perform job duties.

C. Information Technology's Responsibilities:

Upon notification, ensure that access is appropriately assigned, modified and/or promptly terminated when workforce members transfer to other positions or leave DPH.

V. VIOLATIONS:

Failure to comply with this policy may result in disciplinary action up to and including termination of employment or contract.

VI. REFERENCES:

2-364SP, Standard Practice